

IAP12 Rec'd PCT/PTO 19 JUN 2006**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Patent Application of)	
Benoit Chevallier-Mames)	Group Art Unit:
Application No.:)	Examiner:
Filed: June 19, 2006)	Confirmation No.:
For: CRYPTOGRAPHIC MODULAR)	
EXPONENTIATION METHOD)	
PROTECTED AGAINST DPA)	
ATTACKS (As Amended))	

FIRST INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the duty of disclosure as set forth in 37 C.F.R. § 1.56, the accompanying information is being submitted in accordance with 37 C.F.R. §§ 1.97 and 1.98.


To assist the Examiner, the documents are listed on the attached form PTO-1449. It is respectfully requested that an Examiner initialed copy of this form be returned to the undersigned.

Respectfully submitted,

BUCHANAN INGERSOLL PC

Date: June 19, 2006

By:


James A. LaBarre
Registration No. 28632

P.O. Box 1404
Alexandria, VA 22313-1404
703.836.6620

Substitute for form 1449/PTO & 1449B/PTO

IAPI2 Rec'd PCT/PTO 19 JUN 2006

**FIRST
INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(use as many sheets as necessary)

Sheet 1 of 1

Application Number	Unassigned
Filing Date	June 19, 2006
First Named Inventor	Benoit CHEVALLIER-MAMES
Examiner Name	
Attorney Docket No.	1032326-000398

U.S. PATENT DOCUMENTS

Examiner Initials	Document Number	Kind Code (if known)	Name of Patentee or Applicant of Cited Document	Issue/Publication Date (MM-DD-YYYY)

FOREIGN PATENT DOCUMENTS

Examiner Initials	Document Number	Kind Code (if known)	Country	Date of Publication (MM-DD-YYYY)	STATUS						
					Translation	Partial Translation	Eng. Lang. Summary	Search Report	IPER	Abstract	Cited in Spec
	*2 829 646	A1	France	03-14-2003				X			
	*01/31436	A1	WO	05-03-2001				X			

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.
	*CHEVALLIER-MAMES B., "Self-randomized exponentiation algorithms", Topics In Cryptology - CT-RSA 2004, Proceedings, Springer-Verlag, Lecture Notes in Computer Science, Vol. 2964, 02/27/2004, pages 236-249, Berlin, Germany.
	*WALTER C.D., "Mist: An Efficient Randomized Exponentiation Algorithm For Resisting Power Analysis", Lecture Notes In Computer Science, Springer Verlag, New York, New York, Vol. 2271, 02/18/02, pages 53-66.
	*JOYE M., "Recovering Lost Efficiency of Exponentiation Algorithms on Smart Cards", Electronics Letters, IEE Stevenage, GB, Vol. 38, No. 19, 09/12/02, pages 1095-1097.
	*ITOH K. et al., "DPA Countermeasures By Improving The Window Method", Cryptographic Hardware and Embedded System, International Workshop, 08/13/02, pages 303-317.

***Copy Attached**

Examiner Signature	Date Considered
--------------------	-----------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with M.P.E.P. § 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to Applicant.